RFC-0017 Persistent Validation and Assessment Standard

RFC Front Matter

- **Status:** Open
- **Created By:** FedRAMP
- **Start Date:** 2025-09-15
- **Closing Date:** 2025-10-15
- **Short Name:** rfc-0017-persistent-validation

Where to Comment

Members of the public may submit multiple different comments on different issues during the public comment period. The public is asked to please refrain from including documents or spreadsheets (especially those with in-line comments or suggested changes) in public comment as this creates a significant additional review burden.

Formal public comment for official consideration by FedRAMP can be made via the following mechanisms in order of preference:

1. GitHub Post: https://github.com/FedRAMP/community/discussions/88
2. Public Comment Form: https://forms.gle/yYiCUCYt3WruZRBQ6
3. Email: pete@fedramp.gov with the subject "**RFC-0017 Feedback**"

Note: FedRAMP will review and publicly post all public comments received via email, but will not otherwise respond. Email submissions from federal agencies will only be made public when requested by the agency.

Summary & Motivation

Governance, Risk, and Compliance (GRC) should be integrated directly into engineering and security programs within modern cloud services instead of added on at the end by a separate part of the organization with different goals, expectations, and levels of responsibility and accountability. Automation should be used to align engineering teams with security goals and empower them to rapidly develop and deploy changes and capabilities in an environment where secure outcomes are encouraged or enforced by the engineering tools, pipelines, and workflows they normally follow.

In a modern threat environment it simply takes too long and costs too much to make changes at the engineering level then wait for a future audit by entirely separate parts of the organization to review those changes or enforce policies that are not directly informed by engineering. Development and operations teams began to work more closely together fifteen years ago to ensure that decisions made early in the engineering process align with delivery; the only way to scale modern secure systems is to ensure security and compliance is integrated early into the engineering process as well, including native integration into processes and tools wherever possible.

This proposed Persistent Validation and Assessment Standard formalizes the core vision for FedRAMP 20x authorizations that separates 20x from Rev5 by requiring providers to directly and deeply integrate the security and compliance process within their engineering activities instead of tacking GRC onto the end. It also outlined the requirements and recommendations for assessing the capabilities and completeness of persistent validation as the core activity required for FedRAMP 20x authorization.

All FedRAMP 20x Moderate authorizations will be required to demonstrate their commitment to defining security objectives in code and implementing the persistent validation of these objectives within their infrastructure and practices. This standard does create an additional burden for cloud service providers but is designed to deliver clear business value that will incentivize the adoption of secure practices within commercial services instead of building separate government services to follow these practices.

Effective Date(s) & Overall Applicability

This is a draft standard released for public comment; it does not apply to any FedRAMP authorization and MUST NOT be used in draft form.

- FedRAMP **20x**:
  - This standard will initially apply to all FedRAMP 20x authorizations when formalized.
  - Phase One Pilot participants have one year from authorization to fully implement this standard but must demonstrate continuous quarterly progress.
  - Phase Two Pilot participants must demonstrate significant progress towards implementing this standard prior to authorization.
- FedRAMP **Rev5**:
  - This standard DOES NOT apply to FedRAMP Rev5 authorizations.

Documentation Guidelines

The following FedRAMP documentation guidelines apply to this document:

- The capitalized key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in IETF RFC 2119.
- FedRAMP-specific terms defined in FRD-ALL (FedRAMP Definitions) are italicized throughout this document for reference.

Background & Authority

OMB Circular A-130: Managing Information as a Strategic Resource defines continuous monitoring as *“maintaining ongoing awareness of information security, vulnerabilities, threats, and incidents to support agency risk management decisions.”*

The FedRAMP Authorization Act (44 USC § 3609 (a) (7)) directs the Administrator of the General Services Administration to *“coordinate with the FedRAMP Board, the Director of the Cybersecurity and Infrastructure Security Agency, and other entities identified by the Administrator, with the concurrence of the Director and the Secretary, to establish and regularly update a framework for continuous monitoring…”*

Purpose

FedRAMP 20x is built around the core concept that secure cloud service providers will persistently and automatically validate that their security decisions and policies are being implemented continuously within their cloud service offering. The activities and operational state of a secure service should be intentional, understood, documented, and in a state that is always known and understood by the provider.

Secure providers will design their business processes and technical procedures to maximize the use of persistent validation and reporting across the entirety of their cloud service offering. This reduces cost by increasing efficiency, enables fast agile delivery of new capabilities through automation, and prevents unintended drift between the cloud service offering in practice and the business goals for the offering. Secure providers will not be worried when an audit comes around that it might result in unexpected findings and frustration.

All FedRAMP 20x Authorized providers are expected to implement persistent validation programs as part of their core engineering workflow. These programs should be optimized to deliver value to the provider and their engineering teams first and foremost, though agencies and other customers will benefit from the improved security and insight resulting from high quality persistent validation programs.

To obtain and maintain a FedRAMP 20x authorization, providers will be required to have their persistent validation programs assessed regularly for effectiveness and completeness.

Expected Outcomes

- Cloud service providers will operate effective persistent validation programs to always understand the state of their services.
- Assessors will prioritize technical review of validation programs to ensure the quality and effectiveness of a cloud service provider’s security programs are documented accurately.
- Federal agencies will have significantly increased confidence in the quality and effectiveness of cloud service provider’s security programs.

Definitions

FRD-PVA-01

All Necessary Assessors: All entities who participate in the FedRAMP assessment of a *cloud service offering* in the context of a FedRAMP authorization. This always includes FedRAMP and any FedRAMP recognized Third-Party Assessment Organization (3PAO) contracted by a provider to perform a FedRAMP assessment; this does not include agency assessment teams by default as completed FedRAMP assessments are presumed adequate for their use.

FRD-PVA-02

Persistent Validation: The systematic and *persistent* process of validating that *information resources* within a *cloud service offering* are operating in a secure manner as expected by the goals and objectives outlined by the provider for meeting Key Security Indicators.

FRD-PVA-03

Initial FedRAMP Assessment (IFRA): The first full assessment of a *cloud service offering* seeking FedRAMP authorization, coordinated by the provider with *all necessary assessors*, that results in a FedRAMP authorization.

FRD-PVA-04

Persistent FedRAMP Assessment (PFRA): Follow-on assessments of a *cloud service offering* focused on Key Security Indicators, coordinated by the provider with *all necessary assessors*, to maintain a FedRAMP authorization or change its *impact categorization*; this assessment is limited to assessing the *significant changes* made by the provider since the previous assessment.

Requirements

FRR-PVR

These requirements apply ALWAYS to ALL FedRAMP Authorized cloud services based on the current Effective Date(s) and Overall Applicability of this standard.

FRR-PVA-01

Providers MUST maintain simple high-level summaries of at least the following for each Key Security Indicator:

1. Goals for how it will be implemented and validated, including clear pass/fail criteria and traceability
2. The consolidated *information resources* that will be validated (this should be a high-level consolidated summary such as “all employees with privileged access that are members of the Admin group”)
3. The machine-based processes for validation and the *persistent* cycle on which they will be run
4. The human-based processes for validation and the *persistent* cycle on which they will be run
5. Current implementation status

6. Any clarifications or responses to the assessment summary

FRR-PVA-02

Providers MUST *persistently* run automated and non-automated validation processes on the cycle documented in their Key Security Indicators, following the requirements and recommendations outlined in FRR-PVA-TF regarding timeframes for *persistent* validation and reporting; this process is called *persistent validation* and is part of *vulnerability detection.*

FRR-PVA-03

Providers MUST treat failures *detected* during *persistent validation* or failures of the *persistent validation* process as *vulnerabilities* and follow the requirements and recommendations in the FedRAMP Vulnerability Detection and Response Standard for such findings.

FRR-PVA-04

Providers MUST include *persistent validation* activity in the reports on *vulnerability detection* and *response* activity required by the FedRAMP Vulnerability Detection and Response Standard.

FRR-PVA-05

Providers MUST track *significant changes* that impact their Key Security Indicator goals and validation processes while following the requirements and recommendations in the FedRAMP Significant Change Notification Standard; if such *significant changes* are not properly tracked and supplied to *all necessary assessors* then a full *Initial FedRAMP Assessment* may be required in place of the expected *Persistent FedRAMP Assessment.*

FRR-PVA-TF-LO

This section provides guidance on timeframes that apply specifically to FedRAMP Low authorizations for activities required or recommended in this standard; these timeframes are thresholds that secure providers should consistently strive to exceed by significant margins.

FRR-PVA-TF-LO-01

> Providers MUST complete the validation processes for Key Security Indicators of non-machine-based *information resources* at least once every 3 months.

FRR-PVA-TF-LO-02

> Providers MUST complete the validation processes for Key Security Indicators of machine-based *information resources* at least once every 7 days.

FRR-PVA-TF-LO-03

> Providers MUST complete a *Persistent FedRAMP Assessment* at least once every 12 months.

FRR-PVA-TF-MO

This section provides guidance on timeframes that apply specifically to FedRAMP Moderate authorizations for activities required or recommended in this standard; these timeframes are thresholds that secure providers should consistently strive to exceed by significant margins.

FRR-PVA-TF-MO-01

> Providers MUST complete the validation processes for Key Security Indicators of non-machine-based *information resources* at least once every 3 months.

FRR-PVA-TF-MO-02

Providers MUST complete the validation processes for Key Security Indicators of machine-based *information resources* at least once every 3 days.

FRR-PVA-TF-MO-03

Providers MUST complete a *Persistent FedRAMP Assessment* at least once every 9 months.

FRR-PVA-PA

This section provides requirements and recommendations for providers about *Initial FedRAMP Assessment* and *Persistent FedRAMP Assessment* of a *cloud service offering* for a FedRAMP 20x authorization. These assessments are performed by a FedRAMP recognized 3PAO or by FedRAMP directly.

FRR-PVA-PA-01

Providers MUST have the implementation of their goals and validation processes assessed by a FedRAMP recognized Third-Party Assessment Organization OR by FedRAMP directly, AND MUST include the results of this assessment in the *authorization data* for their Key Security Indicators without modification.

FRR-PVA-PA-02

Providers MUST allow a complete assessment of validation procedures (including underlying code, pipelines, configurations, automation tools, etc.) by *all necessary assessors*.

FRR-PVA-PA-03

Providers SHOULD be prepared and willing to provide technical explanations, demonstrations, and proof to *all necessary assessors* regarding their assertions of the technical capabilities they employ to meet Key Security Indicators and to provide validations.

FRR-PVA-PA-04

Providers MUST be responsive to recommendations and requests from FedRAMP during initial assessment and authorization; otherwise they will be removed from authorization review and barred from submitting an updated authorization request for at least six months.

FRR-PVA-PA-05

Providers MAY ask for and accept advice from their third-party assessor during assessment regarding techniques and procedures that will improve the effectiveness, clarity, and accuracy of their validation and reporting procedures for Key Security Indicators, UNLESS doing so might compromise the objectivity and integrity of the assessment (see also FRR-PVA-AA-07).

FRR-PVA-PA-06

Providers MUST include in their *authorization data* a high-level summary of any advice from their third-party assessor that was received and acted upon during assessment.

FRR-PVA-PA-07

Providers MUST consult with FedRAMP, in collaboration with their assessor, if their assessor determines the provider has not maintained sufficient information about *significant changes* to properly scope a *Persistent FedRAMP Assessment.*

FRR-PVA-AA

This section provides requirements and recommendations for assessors about *Initial FedRAMP Assessment* and *Persistent FedRAMP Assessment* of a *cloud service* *offering* for a FedRAMP 20x authorization. These assessments are performed by a FedRAMP approved 3PAO or by FedRAMP directly.

FRR-PVA-AA-01

Assessors MUST evaluate the underlying processes (both machine-based and human-based) that providers use to validate Key Security Indicators; this evaluation should include at least:

1. The effectiveness, completeness, and integrity of automated processes that perform validation
2. The effectiveness, completeness, and integrity of human processes that perform validation
3. The coverage of these processes within the *cloud service offering*, including if all of the consolidated *information resources* listed are being validated

FRR-PVA-AA-02

Assessors MUST evaluate the accuracy of the Key Security Indicator goals against actual implementation of the process to determine whether or not the provider has accurately documented their process.

FRR-PVA-AA-03

Assessors MUST evaluate whether or not the underlying processes are consistently creating the desired security outcome documented by the provider.

FRR-PVA-AA-04

Assessors MUST perform evaluation using a combination of quantitative and expert qualitative assessment as appropriate AND document which is applied to which aspect of the assessment.

FRR-PVA-AA-05

Assessors SHOULD engage provider experts in discussion to understand the decisions made by the provider and inform expert qualitative assessment, and SHOULD perform independent research to test such information as part of the expert qualitative assessment process.

FRR-PVA-AA-06

Assessors MUST NOT rely on screenshots, configuration dumps, or other point-in-time output as evidence EXCEPT when evaluating the accuracy and reliability of a process that generates such point-in-time output.

FRR-PVA-AA-07

Assessors MUST assess whether or not procedures are consistently followed, including the processes in place to assure this occurs; assessors MUST NOT rely solely on the existence of a procedure document for assessing if appropriate processes and procedures are in place

FRR-PVA-AA-08

Assessors MAY share advice with providers they are assessing about techniques and procedures that will improve the effectiveness, clarity, and accuracy of their validation and reporting procedures for Key Security Indicators, UNLESS doing so might compromise the objectivity and integrity of the assessment (see also FRR-PVA-AA-05).

NOTE: This is intended to provide some leeway that allows an assessor to explain when and why something doesn’t make sense or is hard to understand, or to share pro-tips or similar based on previous experience; it does not allow assessors to consult on the security of a system in general during an assessment.

FRR-PVA-AA-09

Assessors MUST deliver a high-level summary of their assessment process and resulting findings for each Key Security Indicator that is intended for inclusion in the provider's *authorization data.*

FRR-PVA-AA-10

Assessors MUST NOT deliver an overall recommendation on whether or not the *cloud service offering* meets the requirements for FedRAMP authorization; this will be determined by FedRAMP based on the assessment findings for each Key Security Indicator.

FRR-PVA-AA-11

Assessors MUST limit the assessment during a *Persistent FedRAMP Assessment* to *significant changes* made by the *cloud service offering* since the most recently completed FedRAMP assessment UNLESS the provider is unable to supply the necessary information to do so.

FRR-PVA-AA-12

Assessors MUST consult with FedRAMP, in collaboration with the provider, if they determine a provider has not maintained sufficient information about *significant changes* to properly scope a *Persistent FedRAMP Assessment.*